Vigenere Idea, How to encrypt/decrypt. Start talk breaking.

Today, Friday - I need to leave a bit early!!!

Plain Text: 60 14 10 13 8 7 19 18

To encrypt: $^{20}U^2F_{20}E_{16}C_{20}F_{20}$

\[
\frac{26, 16, 15, 33, 10, 11, 27, 21, 23}{\mod}
\]

Key: "UCF" 0, 16, 15, 7, 10, 11, 1, 21, 23

A Q P H K L B V X

3 separate shift ciphers cycled
11! separate shift ciphers

(1) Same letter encrypt into different ciphertext letters
(2) Diff plain encrypt into same cipher.
If we "knew" the keylength, then we would know which letters were shifted the same, and hence have partial letter freq info about the plaintext. (Wouldn't have digrams, trigrams, other structure stuff related to consecutive letters.)

Repeated substring length 3 or greater

Plain: THE
HORSE

If we had 6 THE's by pigeonhole principle some 2 of them must line up.

(Prob we have 5 THE's none line up

\[
\frac{\binom{5}{4} \times 3 \times 2 \times 1}{5 \times 5 \times 5 \times 5 \times 5} = \frac{120}{3125} \approx 0.0384
\]

Remarkable prob of spurious match of diff plain text is low.

\[
\begin{align*}
\text{UCF} & \quad 20 \\
\text{HAD} & \quad 2 \text{ times} \\
27 & \quad 2 \text{ times} \\
128 & \quad 1 \text{ time} \\
\text{BCI} & \quad 3 \text{ times}
\end{align*}
\]
Kasiski Test

Find letter positions of repeated cipher text

\[ QRm = 10, 82, 676 \]

Keyword len multiple \( 82 - 10 = 72 \)
Keyword len multiple \( 676 - 82 = 594 \)

\[ 594 = 8 \times 72 + 18 \]
\[ 72 = 4 \times 18 \]

Index of Coincidence

Given a set of items in a single bin (repeat) items, if I randomly pull 2 out of the bin, what is the probability they are same?

10 Skittles, 5 Mtnm, 20 Twix, 15 R.Hats

\[
p(2 \text{ same}) = p(2 \text{ Stk}) + p(2 \text{ Mtn}) + p(2 \text{ Twi}) + p(2 \text{ Hts})
\]

\[
= \frac{10 \times 9}{50 \times 49} + \frac{5 \times 4}{50 \times 49} + \frac{20 \times 19}{50 \times 49} + \frac{15 \times 14}{50 \times 49}
\]
\[
\frac{90 + 20 + 380 + 210}{2450} = \frac{70}{245} = \frac{14}{49} = \frac{2}{7}
\]

\[1C = \sum_{i=1}^{k} \frac{f_i(f_i-1)}{n(n-1)}\]

\[\sum_{i=1}^{k} f_i = n\]

Total # objects

Pretend our candies are English letters!

8% A, 12% E, 1% Z, etc.

\[1C(\text{English}) \simeq 0.0676 \quad 6.76\%
\]

\[1C(\text{Random letters}) \simeq \frac{1}{26} \simeq 3.85\%
\]

1. Guess a keyword length
2. Separate out bins of ciphered text letters
3. Calc 1C for each bin

index array
freq array
mod